

# Penetration Testing & Emotional Work



Deviant Ollam  
(he/him)

AwarenessCon – 2019/11/20



# My Team and I Are Professional Criminals



# We Don't Belong in Here

---



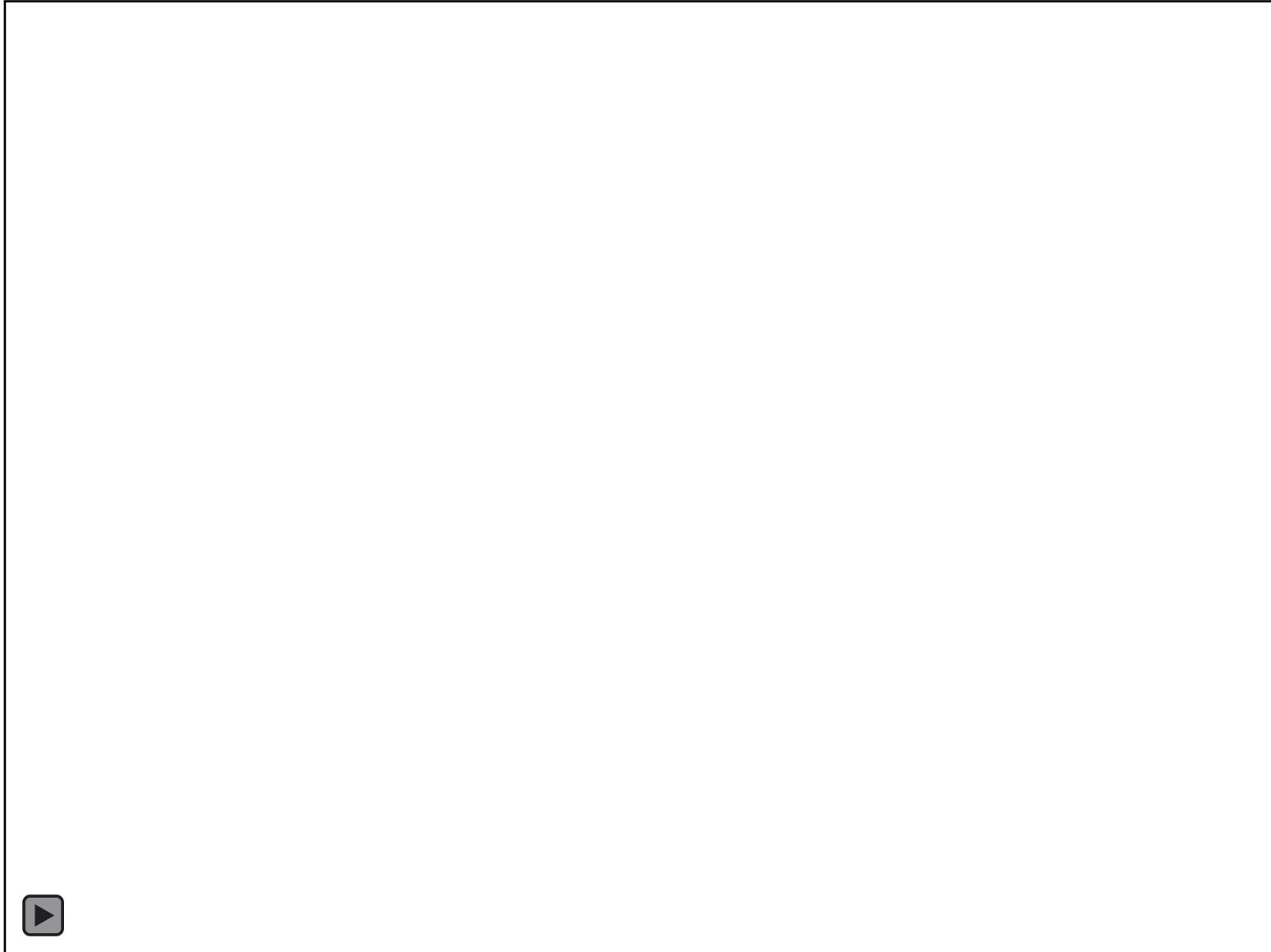


# We Break Into Buildings

---

# We Break Into Buildings

---





# But This Isn't the Best Part of My Job...

---



<https://enterthecore.net>

# ...*This* is the Best Part of My Job

---

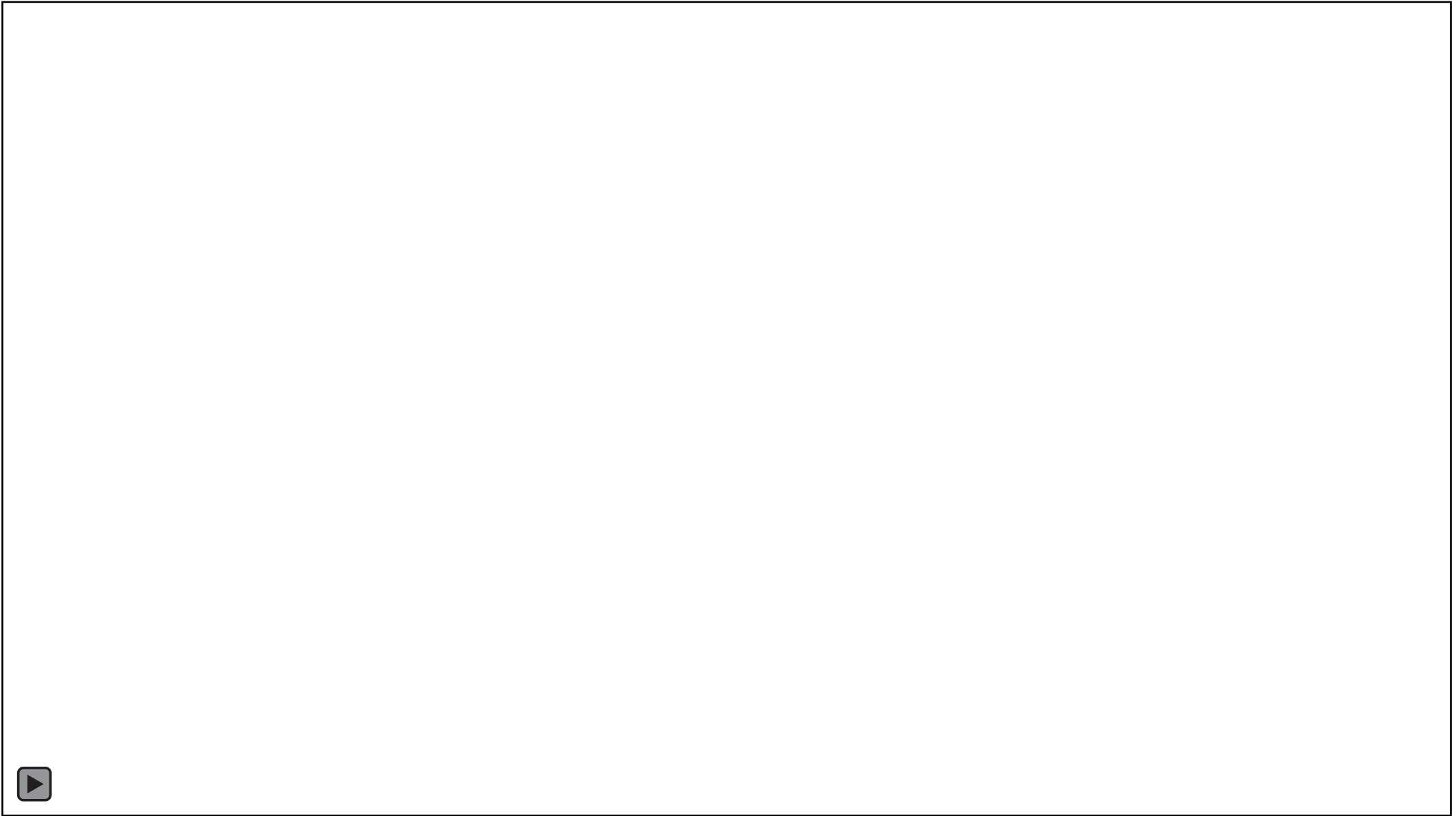


# Another Example: Under Door Attacks



# Under Door Attacks

---





# Under Door Attacks

---

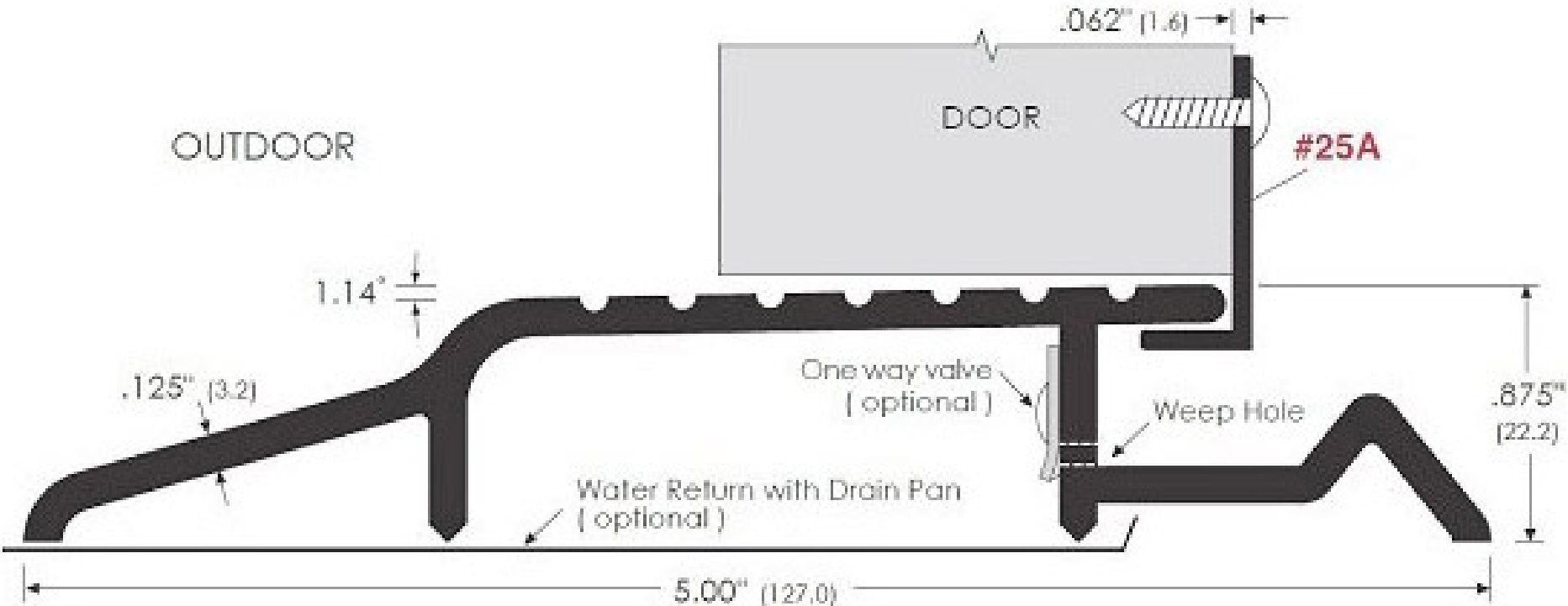


# Mitigation: Interlocking Door Sil Hardware

---



# Mitigation: Interlocking Door Sil Hardware



# Mitigation: Articulating Door Sil Cap

---





# If You Don't Have Any of Those Defenses...

---





# Mitigation: Always Know Where Your Towel Is

---





# Mitigation: Always Know Where Your Towel Is

---



# Another Example: Hinge Pin Removal





# Hinge Pin Removal

---



# Hinge Pin Removal

---





# Hinge Pin Removal

---





# Mitigation: Jamb Pin Screws

---





# Mitigation: Jamb Pin Screws

---





# Mitigation: Jamb Pin Screws

---





# Mitigation: Jamb Pin Screws

---





# Mitigation: Jamb Pin Screws

---



# Another Example: Electronic Attacks





# Stealing Electronic Credentials

---





# Stealing Electronic Credentials

---





# Stealing Electronic Credentials

---





# Stealing Electronic Credentials

---



# Mitigation: RFID Shielding Badge Holders

---





# Attacking RFID Credential Readers

---





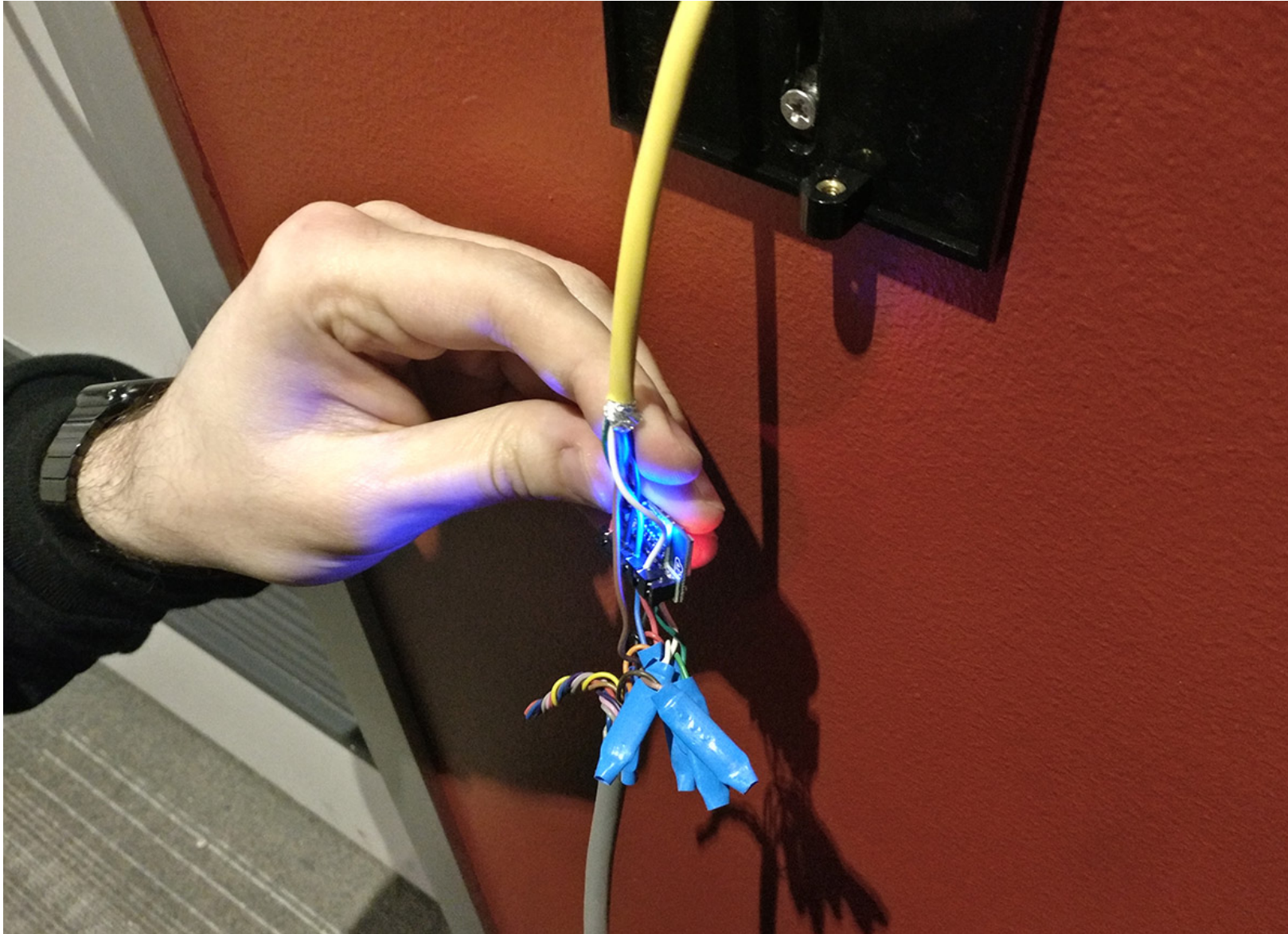
# Attacking RFID Credential Readers

---



# Attacking RFID Credential Readers

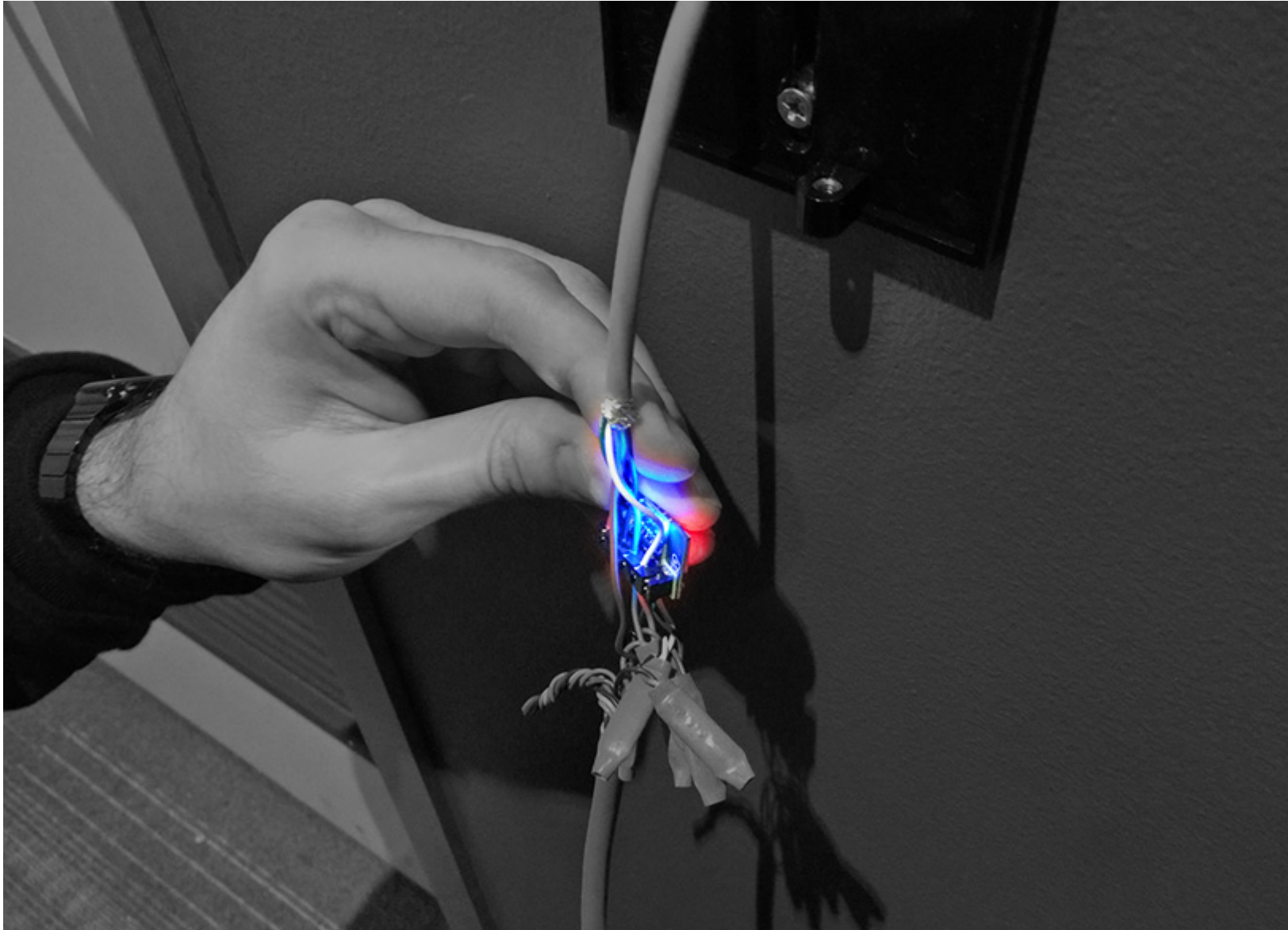
---





# Attacking RFID Credential Readers

---



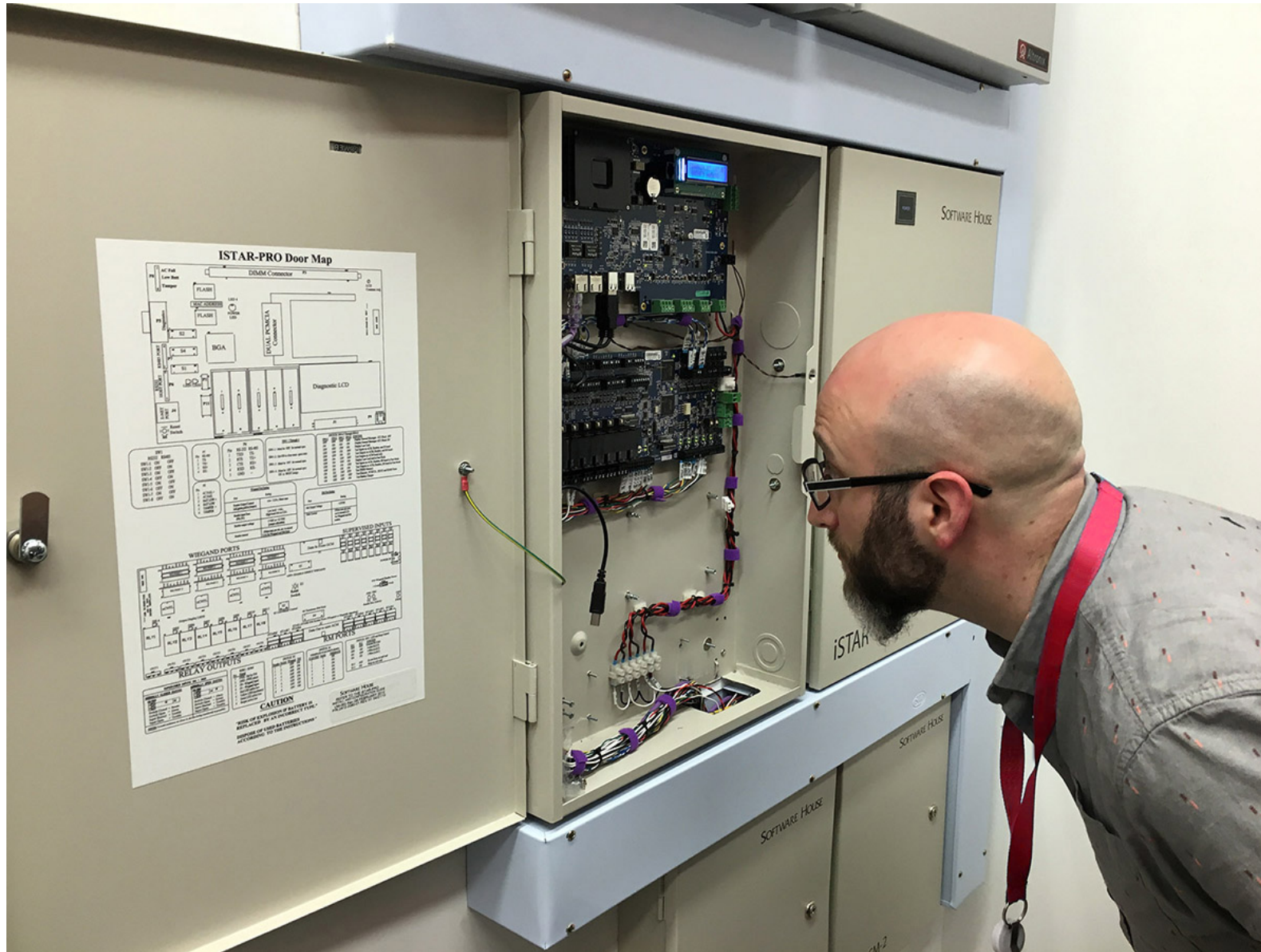
# Attacking RFID Credential Readers

---





# Mitigation: Enabling Access Control Encryption



# Another Example: Electronic Eavesdropping



# We Have Stolen Company Radios

---





# We Use Them to Listen In on Company Communications

---





# We Use Them to Listen In on Company Communications

---



# Another Example: Pretexts and Lying





# “You Don’t Recognize Me? I’m the Elevator Service Tech.”

---



# “We Heard That Your Elevators Were Running Slowly”

---





# “Looks Like We’ve Found the Problem”

---



# “I Need to Check the Elevator Controller Event Logs”

---





# “I’m Totally Legit... Of Course You Can Trust Me”



# Another Example: Destructive Entry





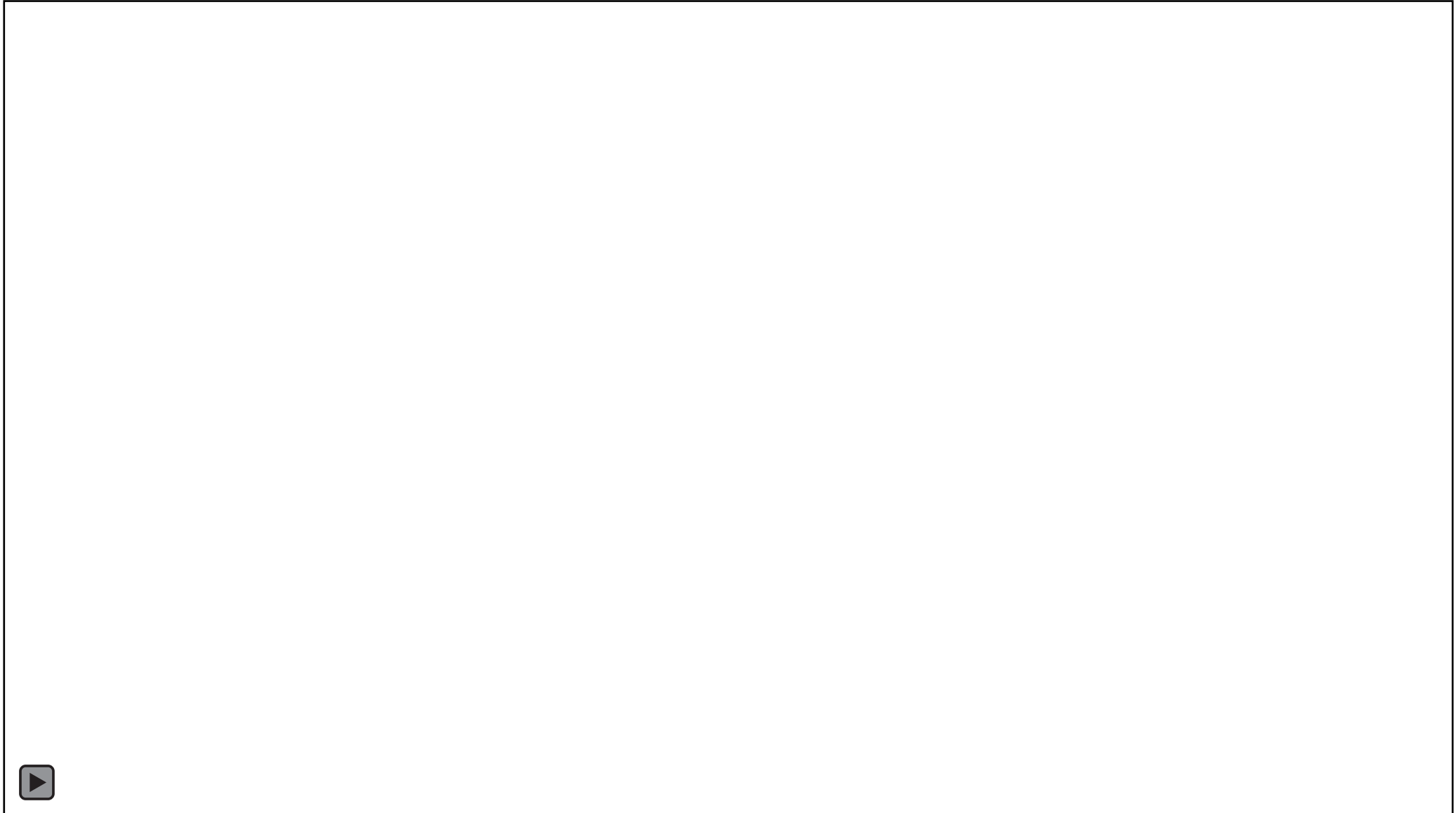
# Yes, My Team Has Used Destructive Methods

---



# Yes, My Team Has Used Destructive Methods

---





# Yes, My Team Has Used Destructive Methods

---



# Of Course, All of This Was Authorized





# My Firm's Contract Language

---

CLIENT is hiring CORE to perform security consulting services. CORE provides computer, systems, and physical security consulting and evaluation services, including penetration-testing services. If the CLIENT wishes to retain CORE to provide security services, including penetration testing on CLIENT's systems, physical security tests, and social engineering attempts against CLIENT's employees, the CLIENT does so understanding that this testing may include the use of methods that a malicious actor may use to damage or disrupt CLIENT's operations. The objective of penetration testing is to identify and report security vulnerabilities to allow the CLIENT to solve those issues in a planned manner before they are exploited by an unauthorized intruder.

# My Firm's Contract Language

---

CLIENT is hiring CORE to perform security consulting services. CORE provides computer, systems, and physical security consulting and evaluation services, including penetration-testing services. If the CLIENT wishes to retain CORE to provide security services, including penetration testing on CLIENT's systems, physical security tests, and social engineering attempts against CLIENT's employees, the CLIENT does so understanding that this testing may include the use of methods that a malicious actor may use to damage or disrupt CLIENT's operations. The objective of penetration testing is to identify and report security vulnerabilities to allow the CLIENT to solve those issues in a planned manner before they are exploited by an unauthorized intruder.



# My Firm's Contract Language

---

CLIENT is hiring CORE to perform security consulting services. CORE provides computer, systems, and physical security consulting and evaluation services, including penetration-testing services. If the CLIENT wishes to retain CORE to provide security services, including penetration testing on CLIENT's systems, physical security tests, and social engineering attempts against CLIENT's employees, the CLIENT does so understanding that this testing may include the use of methods that a malicious actor may use to damage or disrupt CLIENT's operations. The objective of penetration testing is to identify and report security vulnerabilities to allow the CLIENT to solve those issues in a planned manner before they are exploited by an unauthorized intruder.

# How Explicit Are We About Methods and Risks?





# My Firm's Contract Language

---

CORE will perform a physical assessment of the target facility. The assessment is intended to review the existing state of the building's resistance to methods of entry as potentially employed by the designated threat(s) modeled in [ATTACHED DOCUMENT].

While CORE will take reasonable precaution to prevent the following to occur, there is the possibility that any penetration testing may render any attached systems and peripherals unavailable or permanently damaged, including but not limited to servers, network equipment, PCs, elevator systems, HVAC systems, and communication systems.

CLIENT hereby agrees to hold CORE harmless and indemnify them from third party lawsuits arising from CORE's penetration testing on CLIENT's premises.

# My Firm's Contract Language

---

CORE will perform a physical assessment of the target facility. The assessment is intended to review the existing state of the building's resistance to methods of entry as potentially employed by the designated threat(s) modeled in [ATTACHED DOCUMENT].

While CORE will take reasonable precaution to prevent the following to occur, there is the possibility that any penetration testing may render any attached systems and peripherals unavailable or permanently damaged, including but not limited to servers, network equipment, PCs, elevator systems, HVAC systems, and communication systems.

CLIENT hereby agrees to hold CORE harmless and indemnify them from third party lawsuits arising from CORE's penetration testing on CLIENT's premises.



# My Firm's Contract Language

---

CORE will perform a physical assessment of the target facility. The assessment is intended to review the existing state of the building's resistance to methods of entry as potentially employed by the designated threat(s) modeled in [ATTACHED DOCUMENT].

While CORE will take reasonable precaution to prevent the following to occur, there is the possibility that any penetration testing may render any attached systems and peripherals unavailable or permanently damaged, including but not limited to servers, network equipment, PCs, elevator systems, HVAC systems, and communication systems.

CLIENT hereby agrees to hold CORE harmless and indemnify them from third party lawsuits arising from CORE's penetration testing on CLIENT's premises.

# My Firm's Contract Language

---

CORE will perform a physical assessment of the target facility. The assessment is intended to review the existing state of the building's resistance to methods of entry as potentially employed by the designated threat(s) modeled in [ATTACHED DOCUMENT].

While CORE will take reasonable precaution to prevent the following to occur, there is the possibility that any penetration testing may render any attached systems and peripherals unavailable or permanently damaged, including but not limited to servers, network equipment, PCs, elevator systems, HVAC systems, and communication systems.

CLIENT hereby agrees to hold CORE harmless and indemnify them from third party lawsuits arising from CORE's penetration testing on CLIENT's premises.

# “This is Just You Avoiding a Lawsuit”

---





No... This is *Not Just* Legal CYA Language



# My Parents Ran a Dental Practice

---



# My Parents Ran a Dental Practice and Had This Poster...

---

“It wasn’t as bad as  
I thought it would be!”





# Different Spaces... Different Expectations



# Exclusively Client Controlled Spaces



# Zero Potential Concerns

---





# Zero Potential Concerns... Right?

---



# What About An Employee's Office, Desk, or Locker?

---





# What About Legally Sensitive Resources?





# What About Executive Offices?

---



# Shared Spaces



# Vestibules

---





# Lobbies

---



# Stairwells

---





# Elevators

---





# Explicitly Non-Client Spaces



# Other Offices

---



# Other Server Cages

---





# What About Passing “Over” Another Company’s Space?

---



# Building Owner / Landlord Spaces



# Basements

---





# Roofs

---



# Wiring Closets

---





# My Firm's Contract Language

---

If penetration testing services are being requested by CLIENT, CLIENT also authorizes CORE to attempt to access any and all of CLIENT's systems including those systems maintained or controlled by third parties on CLIENT's behalf.

In cooperation with LANDLORD, CLIENT representatives will allow CORE all necessary access to site to assess physical security infrastructure. CORE will work with LANDLORD to meet additional requirements set by LANDLORD in execution of the assessment. LANDLORD will at its option allow or disallow independent third-party validation of common security infrastructure present at the target facility. CORE will attempt to achieve the maximum level of validation within the allowed test parameters.



# My Firm's Contract Language

---

If penetration testing services are being requested by CLIENT, CLIENT also authorizes CORE to attempt to access any and all of CLIENT's systems including those systems maintained or controlled by third parties on CLIENT's behalf.

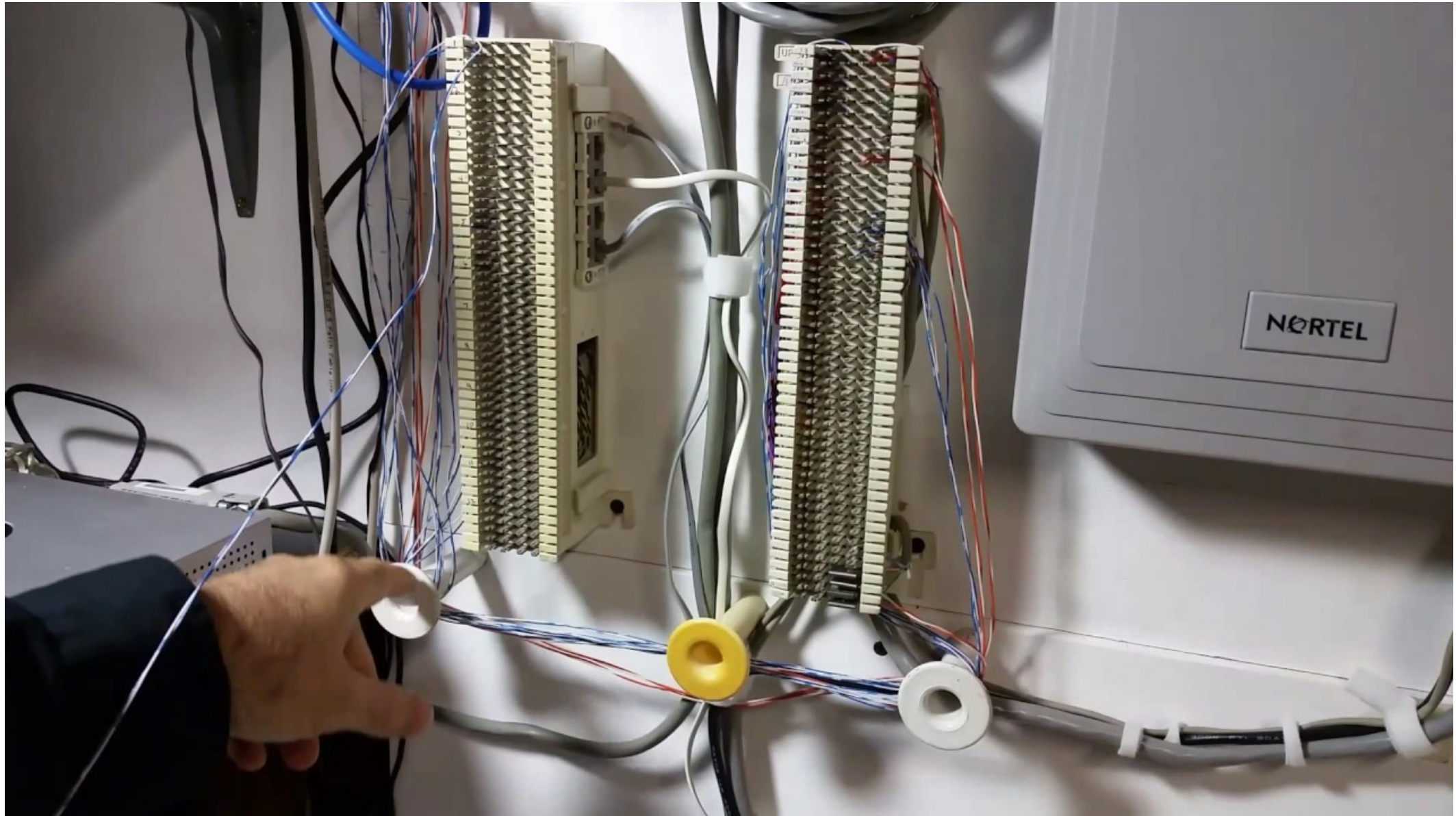
In cooperation with LANDLORD, CLIENT representatives will allow CORE all necessary access to site to assess physical security infrastructure. CORE will work with LANDLORD to meet additional requirements set by LANDLORD in execution of the assessment. LANDLORD will at its option allow or disallow independent third-party validation of common security infrastructure present at the target facility. CORE will attempt to achieve the maximum level of validation within the allowed test parameters.

# Municipal Spaces or Other Authority Control



# Teleco Service Drops / Cross Connect Rooms

---





# FACP / Suppression Rooms





# Elevator Machine Rooms

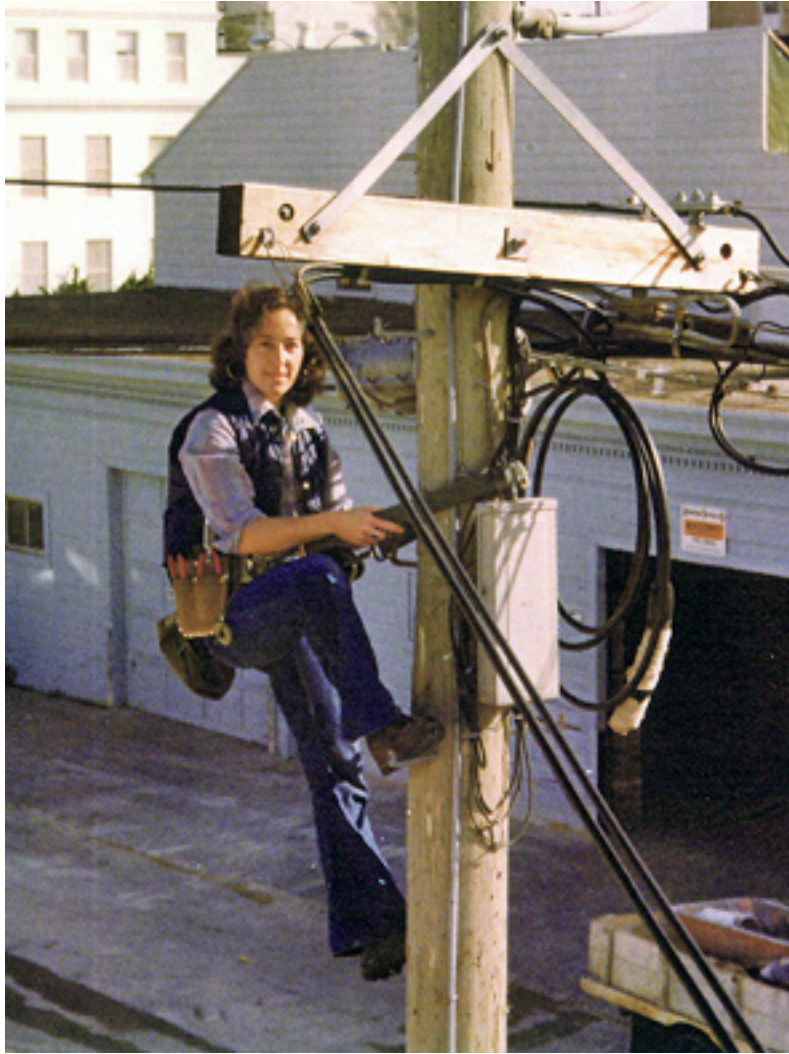
---





# You Might be *Legally* OK, But Someone Else May Get Mad

---





# A Decent Thought Experiment...



# “What if a Janitor Went in There?”

---



# “What if an Electrician Went in There?”

---





# “What if an Emergency Plumber Went in There?”

---



# Expectations, Consent, and Trust



# Some Professionals Whom You Hire Know You Intimately

---





# Penetration Testers See Many Secrets

---



# My Firm's Contract Language

---

CORE recognizes the important nature of keeping CLIENT information confidential and will never divulge trade secrets, proprietary information, or personally identifiable information. Furthermore, the full text of all reports and deliverables regarding the status of CLIENT'S security will not be shared with third parties.

However, in the course of providing similar advice and services to other clients and while training students in physical security classrooms, it may be relevant for CORE to share accounts or lessons learned from their time in the security industry.

CLIENT recognizes that CORE may discuss non-specific summaries of previous work performed and cite examples of how the modern security landscape is most typically approached. CORE shall never reveal specific facts, names, addresses, or any other CLIENT details that are personally-identifiable or would result in a security risk, but CORE may describe certain aspects of their past work for CLIENT in an anonymized and sanitized manner suitable for the education of others.

# My Firm's Contract Language

---

CORE recognizes the important nature of keeping CLIENT information confidential and will never divulge trade secrets, proprietary information, or personally identifiable information. Furthermore, the full text of all reports and deliverables regarding the status of CLIENT'S security will not be shared with third parties.

However, in the course of providing similar advice and services to other clients and while training students in physical security classrooms, it may be relevant for CORE to share accounts or lessons learned from their time in the security industry.

CLIENT recognizes that CORE may discuss non-specific summaries of previous work performed and cite examples of how the modern security landscape is most typically approached. CORE shall never reveal specific facts, names, addresses, or any other CLIENT details that are personally-identifiable or would result in a security risk, but CORE may describe certain aspects of their past work for CLIENT in an anonymized and sanitized manner suitable for the education of others.



# My Firm's Contract Language

---

CORE recognizes the important nature of keeping CLIENT information confidential and will never divulge trade secrets, proprietary information, or personally identifiable information. Furthermore, the full text of all reports and deliverables regarding the status of CLIENT'S security will not be shared with third parties.

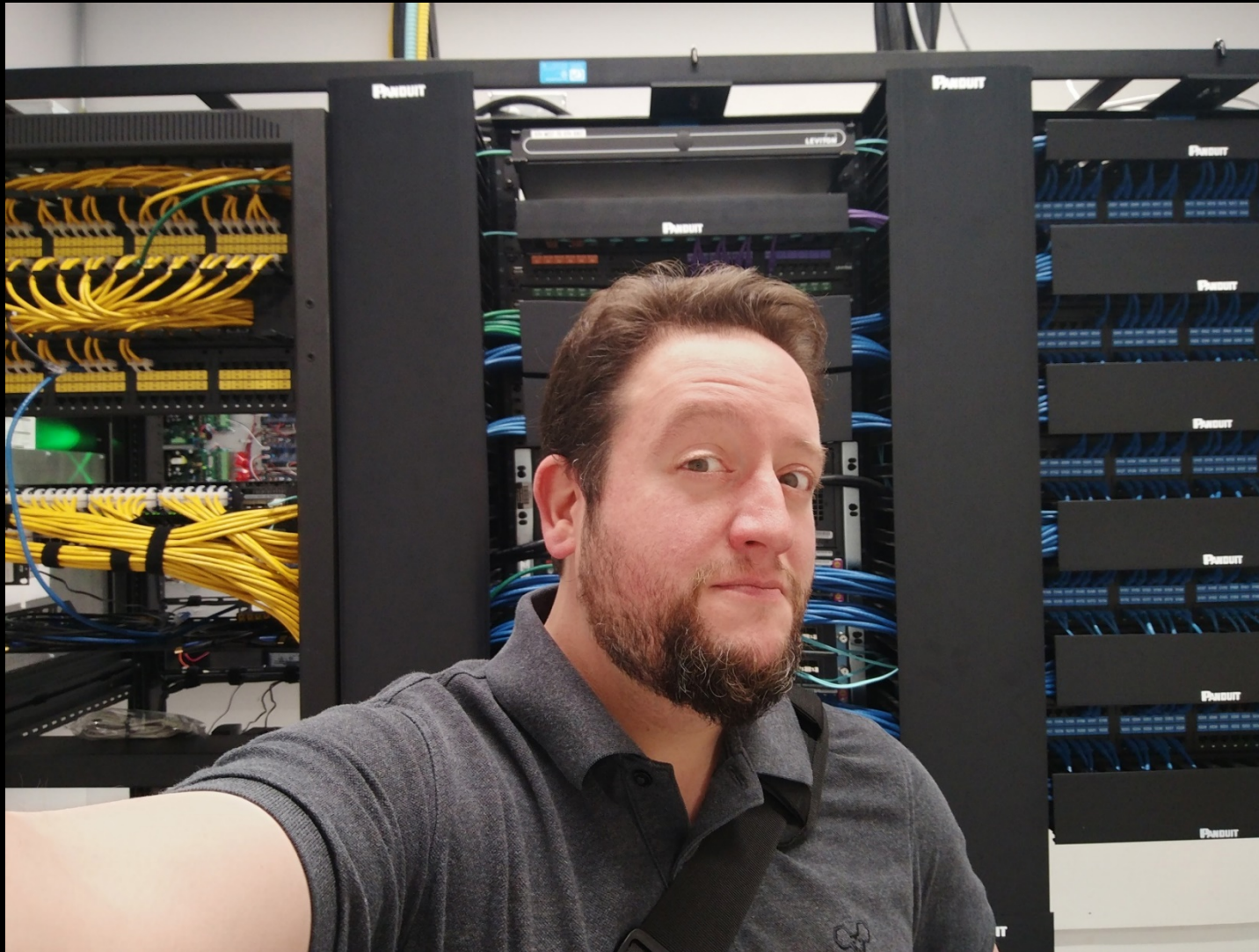
However, in the course of providing similar advice and services to other clients and while training students in physical security classrooms, it may be relevant for CORE to share accounts or lessons learned from their time in the security industry.

CLIENT recognizes that CORE may discuss non-specific summaries of previous work performed and cite examples of how the modern security landscape is most typically approached. CORE shall never reveal specific facts, names, addresses, or any other CLIENT details that are personally-identifiable or would result in a security risk, but CORE may describe certain aspects of their past work for CLIENT in an anonymized and sanitized manner suitable for the education of others.

# Earn Trust... Maintain Trust



# Thank You Very Much



[delta@enterthecore.net](mailto:delta@enterthecore.net)